

Claims

What is claimed is:

- 1 1. A method for maintaining confidential records of an individual comprising the steps of:
 - 3 selecting, by the individual, a record server that is
 - 4 publicly accessible over a network;
 - 5 encrypting a confidential record of the individual;
 - 6 storing the encrypted confidential record on the selected
 - 7 record server; and
 - 8 accessing the encrypted confidential record stored on the
 - 9 selected record server through a defined gateway system.
- 1 2. The method of claim 1 further comprising the step of distributing an access token to a predetermined agent by the individual for use in accessing the stored confidential record over the network.
- 1 3. The method of claim 2 wherein the predetermined agent is a healthcare institution.
- 1 4. The method of claim 1 wherein the confidential record is a medical record.
- 3 5. The method of claim 4 wherein the individual is a patient.

1 6. The method of claim 5 wherein the predetermined agent is
2 the patient who has privileges to read, modify, and annotate the
3 medical record.

1 7. The method of claim 2 further comprising the step of
2 controlling, by the individual, privileges which the
3 predetermined agent has for accessing the confidential record.

1 8. The method of claim 2 further comprising the step of
2 associating a class of agents with a set of privileges for
3 accessing the confidential record, wherein the predetermined
4 agent is a member of the class.

1 9. The method of claim 2 wherein the access token is a private
2 cryptographic key.

1 10. The method of claim 2 wherein the access token is a
2 biometric of the predetermined individual that is measurable by
3 a biometric hardware device.

1 11. The method of claim 2 wherein the access token is a smart-
2 card.

1 12. The method of claim 2 further comprising the step of
2 accessing by the predetermined agent the encrypted confidential

3 record on the record server from any node on the network capable
4 of accepting the access token.

1 13. The method of claim 2 further comprising the step of
2 maintaining anonymity of the individual when the predetermined
3 agent accesses the encrypted confidential record of the
4 individual.

1 14. The method of claim 2 further comprising the step of
2 determining by the individual each portion of the confidential
3 record that is accessible to the predetermined agent.

1 15. The method of claim 1 wherein the gateway system and the
2 record server selected by the individual are the same node on
3 the network.

1 16. The method of claim 1 further comprising the step of
2 defining a schema for representing the confidential record using
3 a markup language.

1 17. In a network, a system for providing access to confidential
2 records of an individual comprising:
3 digital information representing a confidential record of
4 the individual;

5 a publicly accessible server system connected to the
6 network and selected by the individual for storing the
7 confidential record; and

8 a gateway system, in communication with the server system,
9 comprising software for accessing the confidential record of the
10 individual.

1 18. The system of claim 17 further comprising:

2 an access token distributed to a predetermined agent by the
3 individual for use by the gateway system in accessing the stored
4 confidential record.

1 19. The system of claim 18 wherein the access token is a
2 private cryptographic key.

1 20. The system of claim 18 wherein the access token is a
2 biometric of the predetermined agent that is measurable by a
3 biometric hardware device.

1 21. The system of claim 18 wherein the access token is a smart-
2 card.

1 22. The system of claim 17 further comprising a mapper in
2 communication with the gateway system, the mapper associating a
3 predetermined agent with a class of agents that has privileges
4 to access the confidential record.

1 23. The system of claim 22 wherein the predetermined agent is
2 the individual who has privileges to read, write, and annotate
3 the confidential record.

1 24. The system of claim 22 wherein the predetermined agent is a
2 healthcare institution whose privileges to access the
3 confidential record are controlled by the individual.

1 25. The system of claim 17 wherein the gateway system and the
2 record server selected by the individual are the same node on
3 the network.

1 26. The system of claim 17 wherein the confidential record
2 includes a link to an electronic document that is accessible
3 over the network.

1 27. The system of claim 17 wherein the confidential record is a
2 medical record.

1 28. The system of claim 27 wherein the individual is a patient.

1 29. The system of claim 17 wherein the confidential record
2 includes at least one record object, each record object
3 including a privilege section associating a class of agents with
4 a set of privileges for accessing that record object.